Finite Fields and Their Applications **5,** 378–385 (1999)
Article ID ffta.1999.0256, available online at http://www.idealibrary.com on IDEAL®

Primitive Normal Bases for Towers of Field Extensions

Dirk Hachenberger

Institut für Mathematik der Universität Augsburg, 86159 Augsburg, Germany
E-mail: hachenberger@math.uni-augsburg.de

Communicated by Stephen D. Cohen

Received October 12, 1998; revised March 4, 1999

Given an extension E/F of Galois fields and an intermediate field K, we consider the problem whether the (E, K)-trace of a primitive F-normal element of E can be a prescribed F-normal element of K. An interesting application is the existence of trace-compatible sequences of primitive F-normal elements for certain towers of Galois fields. In this respect, particular emphasis is laid on extensions having prime power degree. © 1999 Academic Press

Key Words: finite field; primitive element; normal element (basis); trace compatible sequence.

1. INTRODUCTION

Let $q \geq 2$ be a prime power and $k, e \geq 1$ integers. To (q, k, e) corresponds a triple (F, K, E) of Galois fields: $F = \mathrm{GF}(q)$, and, in a fixed algebraic closure of F, K is the k-dimensional extension over F and E is the e-dimensional extension over K. Let $\mathcal{T}$ denote the set of triples (q, k, e) such that for the corresponding (F, K, E) the following holds: *for every $a \in K$ which is normal over F, there exists a primitive w_a in E which is normal*[1] *over F and whose (E, K)-trace is equal to a.*

Recently, Cohen and the author [CoHa] have proved that for any extension E/F of Galois fields $(E \neq F)$ and for any nonzero $a \in F$ there exists a primitive element w_a in E which is normal over F and whose (E, F)-trace is equal to a. They thereby strengthened the primitive normal basis theorem of Lenstra and Schoof [LeSc] as well as Cohen's theorem on primitive elements

[1] $w \in E$ is called normal over F if its conjugates under the Galois group of E/F form an F-basis of E. For the theory of normal bases we refer to [Ha1].

1071-5797/99 $30.00

with arbitrary trace [Co], and proved a conjecture of Morgan and Mullen [MoMu]. Thus, in the present notation, $(q, 1, e) \in \mathscr{T}$ for all $e \geq 2$ and all prime powers $q \geq 2$.

The motivation for studying the generalization, replacing F by an arbitrary intermediate field K, is that it allows us to prove the existence of trace-compatible sequences of primitive normal elements for certain towers of Galois fields (see Section 6). The following preliminary result indicates that the case $k = 1$ is the easiest instance of the problem considered here.

PROPOSITION 1.1. *Assume that* $(q, k, e) \in \mathscr{T}$. *Then* $(q, \frac{k}{d}, ed) \in \mathscr{T}$ *for every divisor* d *of* k.

Proof. Let d be a divisor of k and $a \in L = \mathrm{GF}(q^\kappa)$ be normal over $F = \mathrm{GF}(q)$, where $\kappa = \frac{k}{d}$. Then there exists a $b \in K = \mathrm{GF}(q^k)$, normal over F, with (K, L)-trace equal to a. As $(q, k, e) \in \mathscr{T}$ by assumption, there exists a $w \in E = \mathrm{GF}(q^{ke})$, primitive in E and normal over F with (E, K)-trace equal to b. The assertion now follows by the transitivity of the trace-mappings. ■

We conclude that "Does $(q, k, e) \in \mathscr{T}$?" is a difficult problem, which for given k is harder, the smaller e is.[2] For example $(q, k, 1) \in \mathscr{T}$ if and only if *every* normal element of $\mathrm{GF}(q^k)$ over $\mathrm{GF}(q)$ is primitive in $\mathrm{GF}(q^k)$. This holds for instance when $(q^k - 1)/(q - 1)$ is a prime (whence necessarily q and k are primes), e.g. $(2, k, 1) \in \mathscr{T}$ for all Mersenne primes $2^k - 1$. This indicates that the case $e = 1$ is hopeless.

If $e = 2$, we can prove that $(q, k, 2) \in \mathscr{T}$ for all $k \geq 1$ whenever q is a power of 2 (see Section 2 for a generalization).

If $e \geq 3$, we can provide a sufficient criterion for "$(q, k, e) \in \mathscr{T}$" (see Section 3), which enables us to prove an asymptotic result (in Section 4), stating that in the range $q \geq 17$, $k \geq 1$ and $e \geq 3$ there are at most finitely many triples which are not members of $\mathscr{T}$.

In Section 5 we shall concentrate on the case where k and e are powers of a prime r and present existence results which hold without any restriction for q.

2. SPECIAL EXTENSIONS

In the present section we consider the case where e is divisible by the characteristic of the underlying fields. Theorem 2.1 generalizes Proposition 2.2 of [CoHa].

THEOREM 2.1. *Let* $q > 1$ *be a prime power and let* $e > 1$ *be an integer which is divisible by the characteristic* p *of* $F = \mathrm{GF}(q)$. *Then* $(q, k, e) \in \mathscr{T}$ *for every* $k \geq 1$.

[2] This corresponds to [CoHa], where extensions of small degree deserved particular attention.

Proof. Write $e = e'\varepsilon$, where ε is a power of p and e' is prime to p, and let E' be the extension of degree ke' over F. An application of Theorem 10.5 of [Ha1] shows that $w \in E$ is normal over F if and only if the (E, E')-trace of w is normal in E' over F. Now, let $a \in K = \mathrm{GF}(q^k)$ be normal over F. Choose an element $v \in E'$ which is normal over F and whose (E', K)-trace is equal to a. By [Co] there exists an element $w \in E$ which is primitive in E and whose (E, E')-trace is equal to v. The first part of the proof asserts that w is normal over F, and the transitivity of the trace mappings implies that w has (E, K)-trace equal to a, whence everything is proved. ■

3. A SUFFICIENT CRITERION

The aim of the present section is to provide a sufficient criterion for (q, k, e) to belong to $\mathscr{T}$ (see Proposition 3.1). It is proved by means of characters and Gauss sums and generalizes Proposition 4.1 of [CoHa]. We omit the proof and refer to [Ha2] instead, where the relevant character sum formulation is given in the course of studying the existence of primitive normal elements with prescribed trace and norm.

Because of Theorem 2.1 we may assume that q and e are relatively prime. Let $Q = q^k$ and

$$t_K := \frac{x^{ke} - 1}{x^k - 1} = \sum_{j=0}^{e-1} x^{kj}. \tag{3.1}$$

Finally, let $\omega = \omega(q, k, e)$ be the number of distinct prime divisors of $Q^e - 1$ and let $\Omega = \Omega(q, k, e)$ be the number of distinct monic irreducible F-divisors of t_K.

PROPOSITION 3.1. *If* $Q^{e/2-1} > (2^\omega - 1)\cdot(2^\Omega - \frac{1}{Q})$, *then* $(q, k, e) \in \mathscr{T}$.

Observe that Proposition 3.1 gives no information for $e = 1$ or $e = 2$. For $e \geq 3$, however, it provides a nontrivial criterion which is further studied in the following section.

4. ASYMPTOTIC RESULTS

Based on Proposition 3.1, we shall here prove asymptotic results for membership of $\mathscr{T}$. Throughout, let again $\omega = \omega(q, k, e)$ and $\Omega = \Omega(q, k, e)$.

THEOREM 4.1. *There are at most finitely many triples* (q, k, e) *with* $q \geq 17$, $k \geq 1$, *and* $e \geq 3$ *which are not members of* $\mathscr{T}$.

Proof. With $n = ke$ we have $\Omega \le n - k$ (see (3.1)). Furthermore, $2^\omega \le d(q^{ke} - 1)$, the latter being the number of positive divisors of $q^{ke} - 1$. By [HaWr, Sec. 18.1, Satz 315], it holds that for any $\varepsilon > 0$ there exists a constant $c_\varepsilon > 0$ such that $2^\omega \le c_\varepsilon q^{n\varepsilon}$. Thus, using Proposition 3.1, for $(q, k, e) \in \mathscr{T}$ it is sufficient that $2^{n-k} c_\varepsilon q^{n\varepsilon} < q^{n/2-k}$. Since $k = \frac{n}{e} \le \frac{n}{3}$ it suffices to have $2^{(2/3)n} c_\varepsilon q^{-(1/6-\varepsilon)n} < 1$. Assume therefore that $\varepsilon < \frac{1}{6}$, and let $\delta := \frac{1}{4} - \frac{3}{2}\varepsilon$. Then $\frac{2}{3}\delta n = (\frac{1}{6} - \varepsilon)n > 0$, whence for $(q, k, e) \in \mathscr{T}$ it is sufficient to have

$$c_\varepsilon \left(\frac{2}{q^\delta} \right)^{(2/3)n} < 1. \tag{4.1}$$

The latter holds, independent of $n = ke \ge 3$, whenever q is large enough, say $q \ge q_\varepsilon$, where q_ε is a constant depending only on ε.

Observe moreover that $\delta < \frac{1}{4}$, whence for $q \ge 17$, the fraction $2/q^\delta$ is less than 1, such that (4.1) is satisfied whenever n is large enough. Thus, if q is from the interval $[17, q_\varepsilon]$ there are only finitely many $n = ke$ such that (q, k, e) is not a member of $\mathscr{T}$, and everything is proved. ■

In order to obtain results of a more concrete nature, one can use Lemma 2.6 of [LeSc], giving rise to a variety of upper bounds for ω. For an integer $l > 1$, let Λ be a set of primes $s \le l$ containing each prime divisor $r \le l$ of $q^{ke} - 1$, and let $L(\Lambda) := \prod_{s \in \Lambda} s$. Then

$$\omega < \frac{ke \log q - \log L(\Lambda)}{\log l} + |\Lambda|.$$

Consequently, if

$$A(q, k, e, l, \Lambda) := \frac{\Omega(q, k, e)}{k} + \frac{1}{k} \cdot \left(|\Lambda| - \frac{\log L(\Lambda)}{\log l} \right) \tag{4.2}$$

and

$$M(e, l) := \frac{e - 2}{\log 4} - \frac{e}{\log l}, \tag{4.3}$$

then the following holds.

LEMMA 4.2. *If* $M(e, l) \cdot \log q \ge A(q, k, e, l, \Lambda)$, *then* $(q, k, e) \in \mathscr{T}$. ■

If $\Omega \le (e - 1)k/d$ for $d \ge 1$, then, for suitable l and Λ, we may replace $A(q, k, e, l, \Lambda)$ in Lemma 4.2 by the larger

$$B_d(k, e, l, \Lambda) := \frac{e - 1}{d} + \frac{1}{k} \cdot \left(|\Lambda| - \frac{\log L(\Lambda)}{\log l} \right) \tag{4.4}$$

and obtain $(q, k, e) \in \mathscr{T}$, if

$$M(e, l) \cdot \log q \geq B_d(k, e, l, \Lambda). \tag{4.5}$$

If Λ_l is the set of all primes $s < l$, then, for $M(e, l) > 0$ the function $B_d(k, e, l, \Lambda_l) M(e, l)^{-1}$ is decreasing when e or k are increasing. We therefore further obtain the following. (Observe that by Theorem 2.1, $\bar{q}$ and $\bar{e}$ may have a nontrivial common divisor.)

PROPOSITION 4.3. *Let $e \geq 3$ be relatively prime to $q, k \geq 1$, and let $l > 1$ be such that $M(e, l) > 0$. If $M(e, l) \cdot \log q \geq B_1(k, e, l, \Lambda_l)$, then $(\bar{q}, \bar{k}, \bar{e}) \in \mathscr{T}$ for all prime powers $\bar{q} \geq q$, all $\bar{k} \geq k$, and all $\bar{e} \geq e$.*

We finally remark that, e.g., $M(e, l) > 0$ for $l > 64$ and $e \geq 3$, or $l > 16$ and $e \geq 4$. If $l = 149$ then Proposition 4.3 shows that $(q, k, e) \in \mathscr{T}$ whenever $q \geq 3104$, $k \geq 4$, and $e \geq 4$.

5. PRIME POWER EXTENSIONS

In the present section, we apply the results of Section 3 and Section 4 to the case where E/F is an extension of prime power degree and prove the following.

THEOREM 5.1. *Let $q \geq 2$ be any prime power, r a prime, and p the characteris of $F = \mathrm{GF}(q)$. Then the following assertions hold.*

(1) *If $r \geq 5$ or if $r = p$ then $(q, r^\alpha, r^\beta) \in \mathscr{T}$ for all $\alpha \geq 0$ and all $\beta \geq 1$.*
(2) *$(q, 3^\alpha, 3^\beta) \in \mathscr{T}$ for all $\alpha \geq 0$ and all $\beta \geq 2$.*
(3) *$(q, 8 \cdot 2^\alpha, 2^\beta) \in \mathscr{T}$ for all $\alpha \geq 0$ and all $\beta \geq 2$.*

We start with the proof of (1). By Theorem 2.1, the assertion holds if $r = p$. Let us therefore assume that $r \geq 5$, $r \neq p$. Since $(q, 1, r) \in \mathscr{T}$ by [CoHa], and by using Proposition 1.1, it remains to show that $(q, r^{n-1}, r) \in \mathscr{T}$ for all $n \geq 2$. Let therefore $k = r^{n-1}$ and $e = r$. Then t_K (see (3.1)) is the r^nth cyclotomic polynomial Φ_{r^n}, and therefore

$$\Omega = \Omega(q, r^{n-1}, r) = \frac{\varphi(r^n)}{\mathrm{ord}_{r^n}(q)} = \frac{r^{n-1}(r-1)}{\mathrm{ord}_{r^n}(q)},$$

where $\mathrm{ord}_{r^n}(q)$ denotes the multiplicative order of q modulo r^n. If $l \geq 17$ then $M(r, l) > 0$ (see (4.3)), and (4.2) specializes to

$$A(q, r^{n-1}, r, l, \Lambda) = \frac{r-1}{\mathrm{ord}_{r^n}(q)} + \frac{1}{r^{n-1}} \cdot \left(|\Lambda| - \frac{\log L(\Lambda)}{\log l} \right). \tag{5.1}$$

Besides the set Λ_l of all primes $s < l$, a suitable choice for Λ will be $\Lambda_l(q, r^\infty)$, the set of all primes $s < l$ which are different from p and where the multiplicative order of q modulo s is a power of r. In the latter case it is important that Λ remains suitable even for changing n. Moreover, as

$$A(q, r^j, r, l, \Lambda_l(q, r^\infty)) \geq A(q, r^i, r, l, \Lambda_l(q, r^\infty)), \qquad \text{if } j \leq i, \tag{5.2}$$

we seek to find the condition in Lemma 4.2 satisfied for the smallest possible exponent $n-1$. Now, if $l = 191$, then $M(e, l)\log q \geq B_1(k, e, l, \Lambda_l)$ is satisfied for all $k \geq 11$, all $e \geq 11$ and all $q \geq 11$ (see Proposition 4.3). Thus, if $q \equiv 1 \bmod r$ it remains to consider the cases $r = 5$ and $r = 7$. If $l = 131$, then $M(r, l)\log q < B_1(r, r, l, \Lambda_l)$ holds only for $q = 8$ if $r = 7$ and $q \in \{11, 16, 31, 41, 61, 71, 81, 101, 121, 131\}$ if $r = 5$, but all these pairs satisfy

$$\log q \geq \frac{A(q, r, r, l, \Lambda_l(q, r^\infty))}{M(r, l)}. \tag{5.3}$$

Hence, (5.2) and Lemma 4.2 imply that $(q, r^{n-1}, r) \in \mathscr{T}$ for all $n \geq 2$ and all (q, r), where $q - 1$ is divisible by r (and $r \geq 5$).

If $q - 1$ is not divisible by r and if $q \geq 5$, we choose $d = 2$ in (4.4). With $l = 131$, a comparison of $M(e, l)$ with $B_2(k, e, l, \Lambda_l)$ shows that it remains to consider the pairs $(q, r) \in \{(7, 5), (8, 5), (9, 5), (13, 5), (17, 5), (19, 5), (23, 5), (5, 7)\}$. All these satisfy (5.3), whence $(q, r^{n-1}, r) \in \mathscr{T}$ for all $n \geq 2$ and all pairs (q, r) under consideration.

If $q = 4$ or $q = 3$, we may choose $d = 3$ for $r \geq 7$. After applying (4.5) (with $l = 68$), it remains to check the four pairs $(3, 5)$, $(3, 7)$, $(4, 5)$, $(4, 7)$. But these satisfy (5.3) (for the same l), whence $(q, r^{n-1}, r) \in \mathscr{T}$ for all $r \geq 5$ and all $n \geq 2$, when $q = 3$ or $q = 4$.

Assume finally that $q = 2$. Choose $l = 68$. If $r \geq 11$, we may choose $d = 4$ for the test with (4.5). The remaining values of r are 5, 7, 11, 13. These satisfy (5.3) and the proof of (1) is complete.

For the proof of (2) and (3), after applying Proposition 1.1 and the fact that $(q, 1, 9) \in \mathscr{T}$ for all q (see [CoHa]), it remains to show that $(q, 3^{n-2}, 9) \in \mathscr{T}$ for all $n \geq 3$, and that $(q, 2^n, 4) \in \mathscr{T}$ for all $n \geq 3$. Here, t_K (see (3.1)) is equal to $\Phi_{r^{n-1}} \cdot \Phi_{r^n}$, whence

$$\Omega = \Omega(q, r^{n-2}, r^2) = \frac{\varphi(r^{n-1})}{\mathrm{ord}_{r^{n-1}}(q)} + \frac{\varphi(r^n)}{\mathrm{ord}_{r^n}(q)},$$

and (4.2) specializes to

$$A(q, r^{n-2}, r^2, l, \Lambda) = \frac{r-1}{\mathrm{ord}_{r^{n-1}}(q)} + \frac{r(\mathrm{r}-1)}{\mathrm{ord}_{r^n}(q)} + \frac{1}{r^{n-2}} \cdot \left(|\Lambda| - \frac{\log L(\Lambda)}{\log l} \right).$$

If $r = 3$, take $l = 83$. Then $M(9, l)\log q < B_1(3, 9, l, \Lambda_l)$ implies $q \leq 25$. All remaining values for q satisfy

$$\log(q) \geq \frac{A(q, 3, 9, l, \Lambda_l(q, 3^\infty))}{M(9, l)}.$$

This completes the proof of (2) as

$$A(q, r^j, r^2, l, \Lambda_l(q, 3^\infty)) \geq A(q, r^i, r^2, l, \Lambda_l(q, 3^\infty)), \qquad \text{if } j \leq i.$$

If $r = 2$, let $l = 293$. Then $M(4, l)\log q < B_1(16, 4, l, \Lambda_l)$ implies $q \leq 178$. For all these q

$$\log(q) \geq \frac{A(q, 16, 4, l, \Lambda_l(q, 2^\infty))}{M(4, l)} \tag{5.4}$$

is satisfied, whence $(q, 16 \cdot 2^a, 4) \in \mathscr{T}$ for all $a \geq 0$, and it remains to consider the triples $(q, 8, 4)$. If $l = 223$ then $M(4, l)\log q < B_1(8, 4, l, \Lambda_l)$ implies $q \leq 517$. Now (5.4) (with 16 replaced by 8) is satisfied for the remaining q except $q \in \{3, 17, 97\}$. Since (3, 8, 4), (17, 8, 4), and (97, 8, 4) satisfy the condition in Proposition 3.1, the proof of Theorem 5.1 is complete. ■

6. TOWERS OF PRIMITIVE NORMAL BASES

We finally discuss interesting applications of Theorem 3.1 and Theorem 5.1. A *tower over a Galois field* F is a set $\mathscr{L}$ of finite extensions over F which is totally ordered by inclusion. Let $\mu_{\mathscr{L}}$ be the minimum degree of an extension E/K, where $K, E \in \mathscr{L}$ such that K is a proper subfield of E. A sequence $w = (w_L)_{L \in \mathscr{L}}$ is called *trace-compatible for* $\mathscr{L}$ if the (E, K)-trace of w_E is equal to w_K for all $E, K \in \mathscr{L}$ such that K is the subfield of E. Furthermore, w is called *normal over* F if w_L is normal in L over F for all $L \in \mathscr{L}$, and w is called *primitive* if w_L is primitive in L for all $L \in \mathscr{L}$.

THEOREM 6.1. *There exists a constant q_0 such that the following holds. If $\mathscr{L}$ is a tower over $F = \mathrm{GF}(q)$ with $F \in \mathscr{L}$ and with $\mu_{\mathscr{L}} \geq 3$, then there exists a trace-compatible sequence for $\mathscr{L}$ which is primitive and normal over F provided that $q \geq q_0$.*

Proof. Enumerate $\mathscr{L}$ such that $L_0 = F$ and L_i is contained in L_j for $i < j$. For $n = 0$ let w_0 be a primitive element of L_0. Assume by induction that $(w_0, w_1, \ldots, w_n)$ is trace-compatible, primitive, and normal for $\{L_0, L_1, \ldots, L_n\}$ over F. As the degree of L_{n+1}/L_n, say e, is at least 3, Theorem 4.1 guarantees the existence of a constant q_0 such that $(q, k, e) \in \mathscr{T}$ whenever $q \geq q_0$ (independently from k). We can therefore extend the sequence by a primitive w_{n+1} in L_{n+1} which is normal over F and whose (L_{n+1}, L_n)-trace is equal to w_n. Now the assertion follows by induction. ■

Our last result can also be proved via induction, yet applying Theorem 5.1. It holds without any restriction on q.

THEOREM 6.2. *Let $F = \mathrm{GF}(q)$ be any finite field with characteristic p and let r be a prime. Let $\delta = 1$ if $r = p$ or $r \geq 5$, let $\delta = 2$ if $r = 3 \neq p$, and let $\delta = 3$ if $r = 2 \neq p$. For an integer $n \geq 0$, in a fixed algebraic closure of F, let $E_{r,n}$ be the extension of degree $r^{\delta n}$ over F, and let $\mathscr{L}_{F,r} = \{E_{r,n} | n \geq 0\}$. Then there exists a trace-compatible sequence w for $\mathscr{L}_{F,r}$ which is primitive and normal over F.*

REFERENCES

[Co] S. D. Cohen, Primitive elements and polynomials with arbitrary trace, *Discrete Math.* **83** (1990), 1–7.

[CoHa] S. D. Cohen and D. Hachenberger, Primitive normal bases with prescribed trace. *Appl. Alg. Eng. Comm. Comp.* **9** (1999), 383–403.

[Ha1] D. Hachenberger, "Finite Fields: Normal Bases and Completely Free Elements," Kluwer Academic, Boston, 1997.

[Ha2] D. Hachenberger, Universal generators for primary closures of Galois fields, submitted for publication.

[HaWr] G. H. Hardy and E. M. Wright, "Einführung in die Zahlentheorie," Oldenbourg, Munich, 1958.

[LeSc] H. W. Lenstra, Jr., and R. J. Schoof, Primitive normal bases for finite fields, *Math. Comput.* **48** (1987), 217–231.

[MoMu] I. H. Morgan and G. L. Mullen, Primitive normal polynomials over finite fields, *Math. Comput.* **63** (1994), 759–765.